

IN THE CLAIMS:

This listing of claims replaces all prior versions, and listings, of claims of this application:

1 - 45. (Canceled)

46. (Previously presented) A method for providing authentication when messages are sent between an electronic communication apparatus and a server according to a synchronization protocol in which a plurality of different authentication methods are available, comprising:

providing an authentication method indicator that specifies an authentication method of the plurality of different authentication methods according to which the authentication is to be executed;

incorporating into a message the authentication method indicator comprising a plurality of authentication capabilities of the communication apparatus among the plurality of different authentication methods;

transmitting said message to said server according to an authentication protocol of the synchronization protocol;

generating, at the server, an integrity key that is encrypted with the public key of the electronic communication apparatus, and an authentication data value comprising an equivalent of an AKA FRESH parameter;

sending the integrity key and the authentication data value to the electronic communication apparatus;

using the integrity key at the electronic communication apparatus to generate MAC values; and

using a hashing function at the electronic communication apparatus to compute a Hashed Method Authentication Code (HMAC) on the message,

wherein the specified authentication method is any of a group comprising Wireless Public Key Identity (WPKI), Wireless Identity Module (WIM) authentication.

47. (Previously presented) The method according to claim 46, wherein the authentication method indicator is incorporated into a meta command of the synchronization protocol.

48. (Previously presented) The method according to claim 46, wherein the message is an initialization message, and the authentication capabilities of the electronic communication apparatus is indicated in an authentication method list of the initialization message, which is sent to the server for establishing a connection.

49. (Previously presented) The method according to claim 46, wherein any authentication data relating to the specified authentication method is incorporated in a data string of the message sent according to the synchronization protocol.

50. (Previously presented) The method according to claim 46, wherein the authentication method is Global System for Mobile communications (GSM) Subscriber Identity Module (SIM) authentication.

51. (Currently amended) The method according to claim 46, wherein the authentication method is Universal Mobile telephone System (UMTS) Universal Subscriber Identity Module (USIM) authentication, which provides server authentication.

52. (Canceled)

53. (Previously presented) The method according to claim 46, wherein the authentication method is SecureId or SafeWord authentication.

54. (Previously presented) The method according to claim 48, further comprising:

determining at the server the authentication capabilities of the electronic communication apparatus based on the plurality of authentication capabilities listed in the authentication method list.

55. (Previously presented) The method according to claim 54, further comprising:
executing at the server authentication operations according to one of the plurality of authentication capabilities indicated in the authentication method list;
preparing a message at the server comprising the authentication method indicator and any authentication data relating to the specified authentication method; and
transmitting the message to the electronic communication apparatus.

56. (Previously presented) The method according to claim 55, further comprising:
receiving the message at the electronic communication apparatus;
executing, at the electronic communication apparatus, authentication operations according to the authentication method indicated by the authentication method indicator to generate an expected result;
preparing a response to the server comprising the authentication method indicator, and any authentication data; and
transmitting the response to the server.

57. (Previously presented) The method according to claim 46, wherein the authentication method is Subscriber Identity Module/Universal Subscriber Identity Module (SIM/USIM) authentication, the method further comprising:

using CKs/IKs (cipher keys/integrity keys) generated by the electronic communication apparatus and the server, respectively, to provide integrity protection, wherein the CKs/IKs are used for generating MAC values; and
using a hashing function for computing a Hashed Method Authentication Code (HMAC) on the message.

In re: Gustavsson et al.
Application No.: 10/506,943
Filed: March 7, 2005
Page 5

58-75. (Canceled)